DISINFORMATION

A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS

HEARINGS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

30 MARCH 2017, 2PM, HART OFFICE BUILDING

INTELLIGENCE.SENATE.GOV/HEARINGS/OPEN-HEARING-INTELLIGENCE-MATTERS-1

Thomas Rid*

Understanding "cyber operations" in the 21st century is impossible without first understanding intelligence operations in the 20th century. Attributing and countering disinformation operations today is therefore also impossible without first understanding how the US and its European allies attributed and countered thousands of active measures throughout the Cold War.

Active measures are semi-covert or covert intelligence operations to shape an adversary's political decisions. Almost always active measures conceal or falsify the *source*—intelligence operators try to hide behind

* Professor of Security Studies, King's College London. @RIDT

anonymity, or behind false flags. Active measures may also spread forged, or partly forged, *content*. The most concise description of disinformation as an intelligence discipline comes from one of its uncontested grandmasters, Colonel Rolf Wagenbreth, head of the East German Stasi's Active Measures Department X for over two decades:

> A powerful adversary can only be defeated through [...] a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies [...] and within their elites.[1]

The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into *pre-existing* cracks: the more polarized a society, the more vulnerable it is—America in 2016 was highly polarized, with myriad cracks and fissures to drive wedges into. Not old wedges, but improved high-tech wedges that allowed Moscow's operators to attack their target faster, more reactively, and at far larger scale than ever before.

Yet there was one big problem. The Russian disinformation operators also left behind more clues and traces than ever before. Thus the evidence implicating Russian intelligence in hacking-and-leaking operations over the past two years is also more granular than ever before. This digital forensic evidence can only adequately be assessed by looking at the wider picture of the 2016 influence campaign against the US election.

First: *in the past 60 years, active measures became the norm*. Russia's intelligence services pioneered *dezinformatsiya* in early twentieth century. By the mid-1960s, disinformation—or active measures—were well-resourced and nearly on a par with collection in the KGB, the Stasi's HVA, the Czechoslovak StB, and others. The Cold War saw more than 10,000 individual Soviet bloc disinformation operations.[2] The pace of Russian operations subsided during a short lull in the early 1970s, followed by an all-time high-water mark in the mid-1980s, and then a long intermission throughout the 1990s. Only in the late 2000s did disinformation begin to pick up speed again. By 2015 and especially 2016, the old playbook had been successfully adapted to a new technical environment.

Second, *in past 20 years, aggressive Russian digital espionage campaigns became the norm*. The first major state-on-state campaign was MOONLIGHT MAZE, which started in late 1996.[3] Ten years later American and European intelligence agencies and soon also an expanding number of private sector companies were tracking at least three different hacking groups linked to Russia's main intelligence agencies: tracking their implants and tools, their

infrastructure, their evolving methods of operation, their targeting behavior, their evolving operational security, and—perhaps most importantly—the mistakes the Russian operators made again and again. In 2014 a shift in tactics became apparent especially in military intelligence: a once careful, risk-averse, and stealthy espionage actor became more and more careless, risk-taking, and error-prone. One particularly revealing operational security slip-up resulted in a highly granular view of just one slice of GRU[4] targeting between 16 March 2015 and 17 May 2016—that slice contained 19,300 malicious links, targeting around 6,730 individuals.[5] A high-resolution picture of Russia's digital espionage activities emerged.[6]

Third, *in past 2 years, Russian intelligence operators began to combine the two, hacking and leaking*—or digital espionage and active measures.

By early 2015, GRU was targeting military and diplomatic entities at high tempo, especially defense attachés world-wide. Among the targets are numerous senior US military officers and defense civilians, for example the private accounts of the current chairman of the Joint Chiefs of Staff, General Joseph F. Dunford; Generals Philip Breedlove, Wesley Clark, and Colin Powell; Navy Captain Carl Pistole, or current Assistant Secretary of the Air Force Daniel Ginsberg. Among the diplomatic targets were the current US ambassador to Russia, John F. Tefft; his predecessor Michael McFaul; former Permanent Representatives to NATO Ivo Daalder and Kurt Volker; and well-connected security experts Anthony Cordesman, Julianne Smith, and Harlan Ullman. The targets also included a large number of diplomatic and military officials in Ukraine, Georgia, Turkey, Saudi Arabia, Afghanistan, and many countries bordering Russia, especially their military attachés, all legitimate and predictable targets for a military intelligence agency. Russian intelligence also targeted well-known Russian critics, for example the author Masha Gessen, Garry Kasparov, and Alexei Navalny, as well as the Russia-based hacker group Shaltay Boltai. In early 2015, the same entity often referred to as APT28 or FANCYBEAR had successfully breached not just the German Parliament;[7] the Italian military;[8] but also Saudi Arabia's foreign ministry.

Then, in May and June 2015, the first publicly known large-scale disinformation operation, dubbed "Saudi Cables," tested an innovative tactic: hacking a target, exfiltrating compromising material (*kompromat*), setting up a dedicated leak website under false flag, and then passing files to Wikileaks for laundering and wide distribution.[9] Between June 2015 and November 2016, at least six front organizations sprung up as outlets

for compromised files by GRU: Yemen Cyber Army, Cyber Berkut, Guccifer 2.0, DC Leaks, Fancy Bears Hack Team, and @ANPoland.

Finally, *in past year, the timeline of US-election operations began to align.* In early March, GRU began to train its well-established, semi-automated targeting tools from worldwide military and diplomatic targets to US political targets. Between 10 March and 7 April, GRU targeted at least 109 Clinton campaign staffers with 214 individual phishing emails (with 8 more attempts on 12 and 13 May). 36 times Clinton staffers clicked a malicious link (the success rate of actually breaching the account after a victim clicked this link is 1-in-7). Russian intelligence targeted Jake Sullivan in at least 14 different attempts beginning on 19 March, each time with a different malicious link against two of his email addresses. GRU targeted Hillary Clinton's personal email account at least two times in March, but the available data show that she did not fall for the password reset trick. The military intelligence agency also targeted DNC staffers with 16 emails between 15 March and 11 April, and 3 DNC staffers were tricked into clicking the treacherous "reset password" button on 6 April 2016.

Less than two weeks later, on 19 April, the front website DCLeaks.com was registered as a leak outlet for hacked files.[10] The overlap between individuals hacked by GRU and leaked by "DC Leaks" aligns nearly perfectly: out of 13 named leak victims,[11] the available forensic evidence identifies 12 as targeted by GRU, with a spike of activity in late March 2016 (all US victims except George Soros).[12] The Russian-orchestrated leak operation continued apace during the hot summer of 2016 using, often with small batches of files released in more than 80 individual leaks for the best publicity effect.

The *publicly available* evidence that implicates Russian intelligence agencies in the 2016 active measures campaign is extraordinarily strong. The DNC hack can be compared to a carefully executed physical break-in in which the intruders used uniquely identical listening devices; uniquely identical envelopes to carry the stolen files past security; and uniquely identical getaway vehicles.

Listening devices (*implants*): the DNC intruders reused implants that had been deployed in a very large number of Russian intrusions across many hundreds of targets in dozens of countries over the past decade.[13] The implants shared many common features, among them a specific communication protocol and other modular functionality—comparable to

using the exact same listening device in different buildings without ever publishing the design plans for it.[14]

Getaway vehicle (*command-and-control infrastructure*): Russian intelligence agencies reused command-and-control sites—a common technique comparable to using the same getaway car with identical license plates in a burglary.[15] The infrastructure re-use is not easily forged, and allowed investigators to link the DNC breach to other breaches with high confidence, particularly to the German Bundestag hack, which the German government had already attributed to Russian military intelligence.

Envelopes (*encryption keys*): Russian operators also reused encryption keys across different targets, notably in targeting Ukrainian artillery units deployed against Russia-supported separatists as well as a Democratic organization in Washington, as well as in at least 75 other implants across a large number of targets world-wide.[16] This cryptographic overlap is an exceptionally strong forensic link, comparable to a human fingerprint.

But a narrow technical analysis would miss the main political and ethical challenges. Soviet bloc disinformation specialists perfected the art of exploiting *unwitting agents*.[17] In early 1980s, for example, there was no contradiction between being a genuine, honest, innocent peace activist against NATO's Double Track Decision—and at the same time being an unwitting agent for the Soviet cause. The internet has made unwitting agents more potent, more persistent, and more pervasive.

Three different types of unwitting agents stand out in the 2016 campaign. The first is Wikileaks. During the 2016 influence operation Russian intelligence agencies have abused anonymity tools for hacking[18]—and for leaking. Wikileaks was purpose-created to anonymize leaks. The controversial platform is a dream-come-true for active measures operators. Those Russian intelligence officers tasked with utilizing Wikileaks will likely play by their old playbook: any unwitting agent is more effective when left in the belief that they are genuinely holding the moral high-ground, not representing an authoritarian intelligence agency.

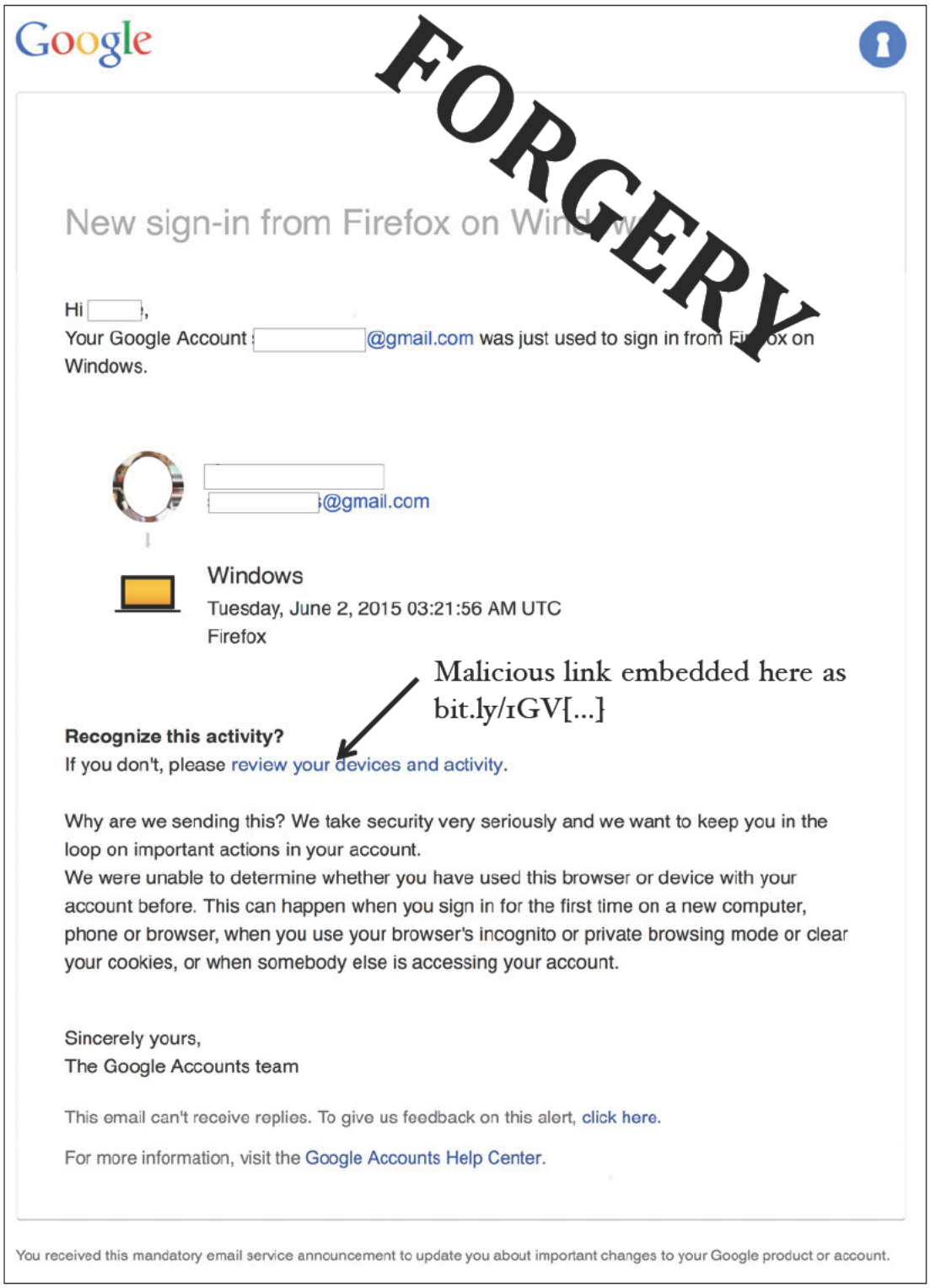
The second major unwitting agent has been Twitter, the social media platform most influential among opinion-leaders. Fully automated bots as well as semi-automated spam and trolling accounts make up a sizeable part of Twitter's active user base.[19] The company could easily generate statistics on how many accounts are automated bots or semi-automated to amplify disinformation or bully opponents; how many interactions and

engagements with politically influential accounts during the 2016 campaign were actual human; and likely how many of those engagements were controlled from abroad or deliberately obfuscated. But the social media firm has a commercial incentive to hide or understate these figures, as they inflate the active user numbers, a precious measure for social media companies. The result is a platform practically purpose-built for active measures: easy exploitation—high impact.

The third group of unwitting agents of 2016 were those journalists who aggressively covered the political leaks while neglecting or ignoring their provenance. Soviet bloc active measures have skillfully fed forgeries and selected documents to journalists many hundreds of times. But doing so required handiwork and craftsmanship: preparing documents; writing cover letters; trust-building; or covert and cumbersome surfacing operations. Cold War disinformation was artisanal; today it is outsourced, at least in part—outsourced to the victim itself. American journalists would dig deep into large dumps, sifting gems, mining news, boosting ops.

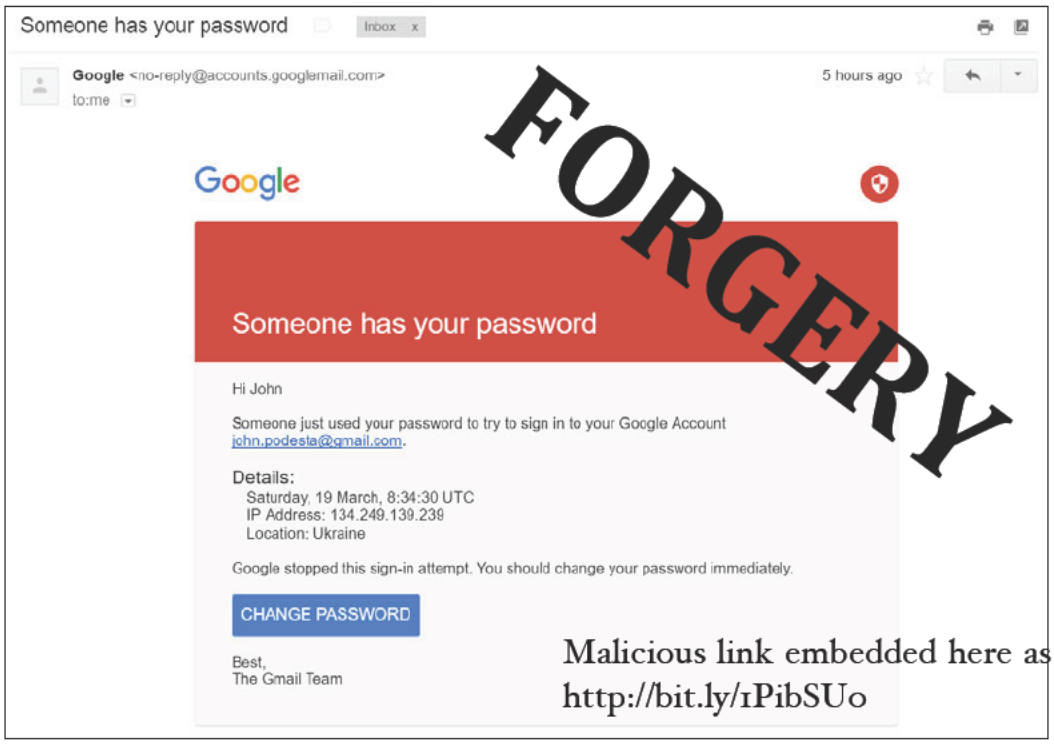
"Sometimes I am amazed how easy it is to play these games," said the KGB's grandmaster of *dezinformatsiya*, General Ivan Agayants, during an inspection of the particularly aggressive active measures shop in Prague in 1965, "if they did not have press freedom, we would have to invent it for them."[20] — Three years later the operator Agayants was speaking with would defect to the US. In 1980 Ladislav Bittman testified on Russian Active Measures here in Congress. "The press should be more cautious with anonymous leaks," Bittman told the Permanent Select Committee on Intelligence, "Anonymity is a signal indicating that the Big Russian Bear might be involved."

Exhibit 1



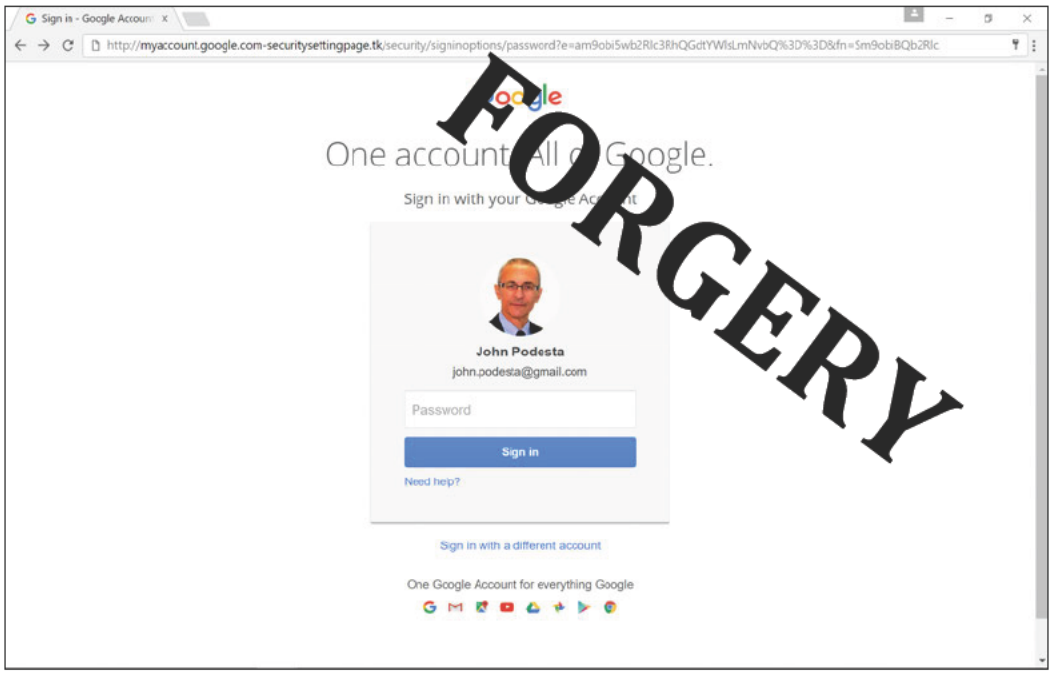
Sample GRU aka APT28/FANCYBEAR phishing email sent on 2 June 2015 (original).

Exhibit 2



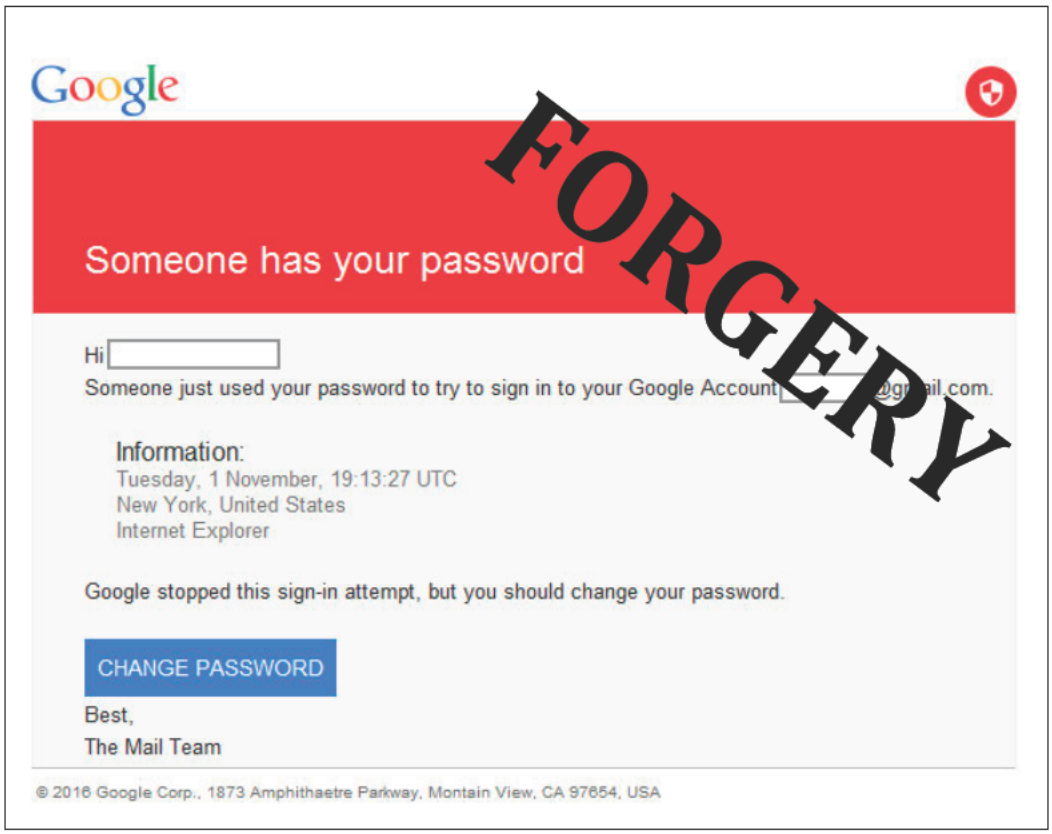
Phishing email sent to John Podesta (reconstruction by Matt Tait). Note the tradecraft: the "o"s in "someone has your password" are unicode homoglyphs, presumably to evade Google's spam filters.

Exhibit 3



Password credential harnessing site, prefilled with John Podesta's picture, name, and email-address. Note the deceptive URL, with a dash, not a forward slash, after google.com, thus pointing to com-securitysettings.tk (reconstruction by Matt Tait).

Exhibit 4

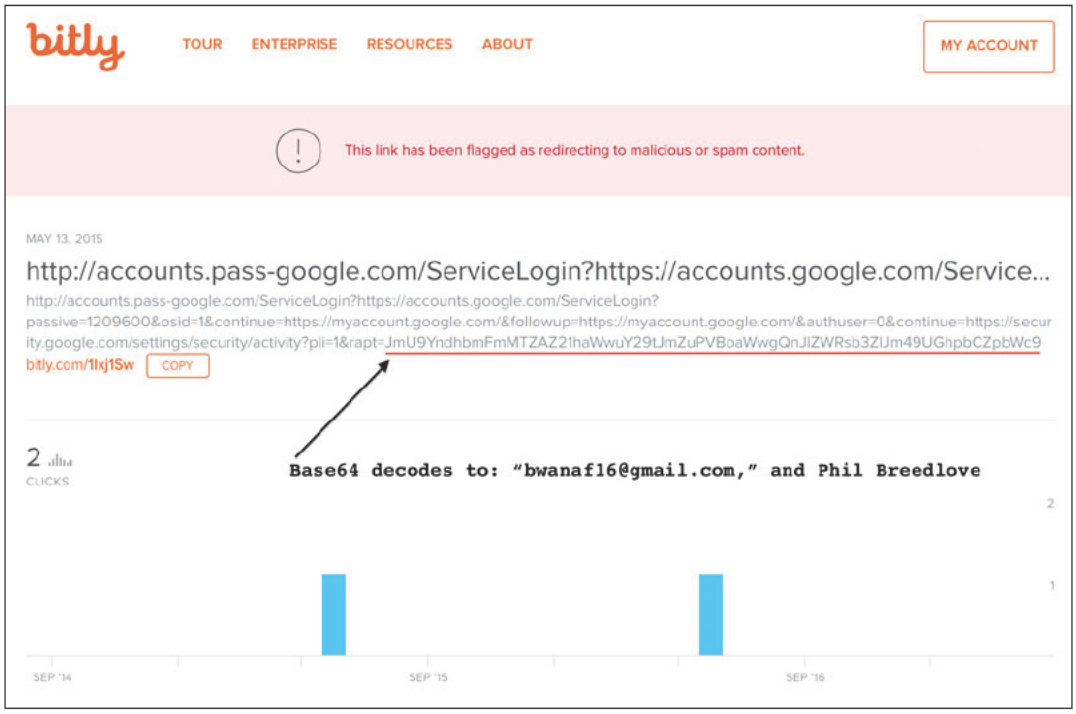


APT28/FANCYBEAR phishing email that fairly accurately represents legitimate warnings from Google. Note the flawed spelling in the address footer. This email was in fact sent from a yandex.com address but made to appear as a Google address. It included a TinyURL-shortened link on the "CHANGE PASSWORD" button (original).

Exhibit 5

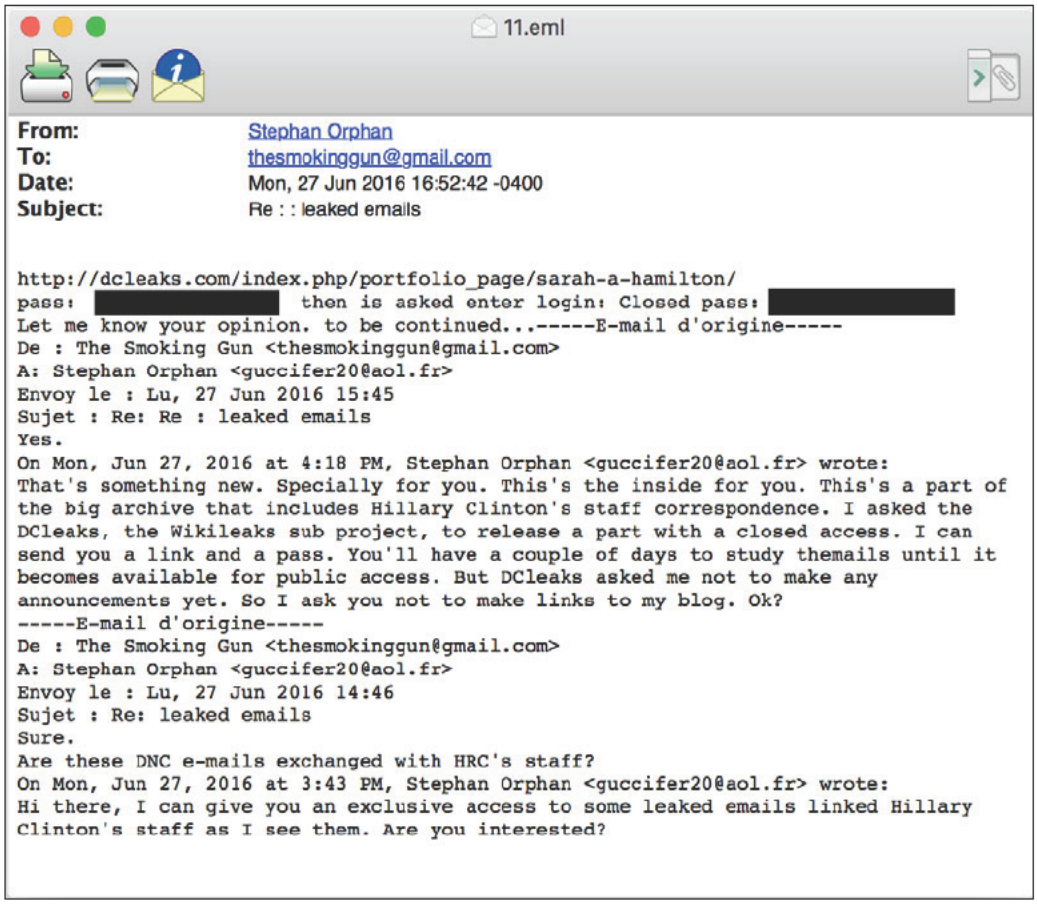
Here APT28/FANCYBEAR, a state-backed attacker, sent a phishing email camouflaging as a state-backed attackers warning. Notably Google's legitimate message is only displayed in the Gmail user interface and never sent via email. This email was sent from a mail.com address, and included a TinyURL-shortened link on the "Change password" link (original).

Exhibit 6



The Russian phishing URL with General Philip M. Breedlove's private email address and name encoded to pre-fill the forged login form. Breedlove was likely compromised in mid-May 2015, less than two weeks after ending his service as Supreme Allied Commander Europe. He became the first leak victim on DC Leaks in June 2016.

Exhibit 7



11.eml

From: Stephan Orphan
To: thesmokinggun@gmail.com
Date: Mon, 27 Jun 2016 16:52:42 -0400
Subject: Re : : leaked emails

http://dcleaks.com/index.php/portfolio_page/sarah-a-hamilton/
pass: [redacted] then is asked enter login: Closed pass: [redacted]
Let me know your opinion. to be continued...-----E-mail d'origine-----
De : The Smoking Gun <thesmokinggun@gmail.com>
A: Stephan Orphan <guccifer20@aol.fr>
Envoy le : Lu, 27 Jun 2016 15:45
Sujet : Re: Re : leaked emails
Yes.
On Mon, Jun 27, 2016 at 4:18 PM, Stephan Orphan <guccifer20@aol.fr> wrote:
That's something new. Specially for you. This's the inside for you. This's a part of the big archive that includes Hillary Clinton's staff correspondence. I asked the DCleaks, the Wikileaks sub project, to release a part with a closed access. I can send you a link and a pass. You'll have a couple of days to study themails until it becomes available for public access. But DCleaks asked me not to make any announcements yet. So I ask you not to make links to my blog. Ok?
-----E-mail d'origine-----
De : The Smoking Gun <thesmokinggun@gmail.com>
A: Stephan Orphan <guccifer20@aol.fr>
Envoy le : Lu, 27 Jun 2016 14:46
Sujet : Re: leaked emails
Sure.
Are these DNC e-mails exchanged with HRC's staff?
On Mon, Jun 27, 2016 at 3:43 PM, Stephan Orphan <guccifer20@aol.fr> wrote:
Hi there, I can give you an exclusive access to some leaked emails linked Hillary Clinton's staff as I see them. Are you interested?

An operational security slip-up from 27 June 2016 in which one front account, Guccifer 2.0, offers non-public access credentials (password redacted) belonging to another front account, DC Leaks, to *The Smoking Gun*. The operators thus provided another forensic artifact to link the two fronts to each other, and to the wider Russian active measures campaign of 2016. Source: "Does a BEAR Leak in the Woods?" *ThreatConnect Research Team*, Arlington, VA: ThreatConnect, 12 August 2016.

Exhibit 8

The likely APT28/FANCYBEAR front website Wikisaleaks.com, captured on 10 August 2015, with the note that files had been provided to Wikileaks. The full-length site is depicted on the right. The captured version is at http://web.archive.org/web/20150810005744/http://www.wikisaleaks.com/

Endnotes

---

[1] Günter Bohnsack, Herbert Brehmer, *Auftrag Irreführung*, Carlsen, 1992, p. 16.

[2] Lawrence Martin (Ladislav Bittman), in interview with Thomas Rid, 25 March 2017, Rockport, MA. See also Bittman, Ladislav, *The Deception Game*, Syracuse University Research Corporation, 1972.

[3] Thomas Rid, *Rise of the Machines*, New York: Norton, 2016, last chapter.

[4] Three of the most potent Western intelligence communities agree with the APT28/FANCYBEAR attribution to Russian military intelligence: the United States; Germany; and the United Kingdom.

[5] SecureWorks shared the full dataset with the author. See also "Threat Group 4127 Targets Hillary Clinton Presidential Campaign," *SecureWorks Counter Threat Unit*, 16 June 2016, as well as "Threat Group-4127 Targets Google Accounts," *SecureWorks Counter Threat Unit*, 26 June 2016.

Out of 19,315 malicious links sent, 3,134 were clicked at least once—just above 16 percent. If the password harvesting success rate is 1-in-7, then the total number of compromised accounts in this set would be around 470, which would mean an overall success rate of 2.4 percent. This estimate is conservative, as the total number of clicks is understated for technical reasons.

[6] The number of private sector reports on the entity codenamed APT28, FANCYBEAR, Sofacy, Sednit, Pawn Storm, STRONTIUM is in the three digits, many of them unfortunately not publicly available. One of the first public reports was *APT28: A Window into Russia's Cyber Espionage Operations?* Milpitas, CA: Fireeye, 27 October 2014.

[7] See "Deutsche Beamte beschuldigen russischen Militärgeheimdienst," *Der Spiegel*, 30 January 2016. Also: "Nachrichtendienstlich gesteuerte elektronische Angriffe aus Russland," *BfV Newsletter*, Beitrag Spionageabewehr, January 2016.

[8] Stefano Maccaglia, "Evolving Threats: dissection of a Cyber- Espionage attack," Abu Dhabi: RSA Conference, November 2015.

[9] Brian Bartholomew and Juan Andrés Guerrero-Saade, "Wave your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks," *Virus Bullentin Conference*, 6 October 2016. (For a more extensive analysis: "TLP Amber" report from autumn 2015 by a major security company, https://www.us-cert.gov/tlp). The attribution of this Saudi operation is particularly difficult. I would assess with moderate confidence that "Wikisaleaks" was a Russian intelligence operation and that Yemen Cyber Army was a Russian front.

[10] For registration information, see http://whois.domaintools.com/dcleaks.com

[11] American victims whose personal emails were subsequently leaked on DC Leaks are Philip Breedlove, Sarah Hamilton, Brian Keller, Zachary Leighton, Capricia Marshall, Ian Mellul, Beanca Nicholson, Carl Pistole, Colin Powell, Sarah Stoll, William Rinehart, and John Podesta (where GRU used Wikileaks as an outlet).

[12] John Podesta was targeted on 19 March; Rinehart on the 22nd; Hamilton, Leighton, Nicholson, and Mellul on the 25th.

[13] Google reported that "Portions of the X-Agent code base can be found in malware dating back to at least 2004," see Neel Mehta, Billy Leonard, Shane Huntley, "Peering into the Aquarium," Palo Alto: Google Security Team, 5 September 2014, p. 20.

[14] The APT28/FANCYBEAR communication protocol is a strong forensic link between breaches against Washington-based political organizations, the compromised app used against Ukraine artillery units, the German Bundestag breach, and other operations. The full source code of the so-called X-Agent implant in question was not publicly available by 27 March 2017. Crowdstrike's Adam Myers, interview with author, Washington, DC, 27 March 2017. See Exhibit 1 for GRU's X-Agent communication protocol.

[15] One example is a re-used IP address, 176.31.112[.]10, which was hardcoded into two DNC implant samples:
4845761c9bed0563d0aa836133111191e075a9b58861e80392914d61a21bad976, and
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f;
as well as in the Bundestag sample,
730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5dc40cbcfb15e1702ed9a.

[16] The 50-bytes RC4 keys had a 46-bytes overlap. The keys were hardcoded into the X-Agent implants that were deployed against the Linux server of a Washington-based political organization—and against Android devices of Ukrainian artillery units in Eastern Ukraine. A member of the 55th Artillery Brigade developed a legitimate targeting app, named Попр-Д30.apk, in early 2013. By late April 2013 a rigged version of that app was offered for download on social media platforms used by the artillery units; this compromised app contained the implant with the similar RC4 key. Below the Linux 50-bytes key, followed by the Android key, with 46 bytes overlap (non-overlapping bytes in square brackets):

3B C6 73 0F 8B 07 85 C0 74 02 FF [D0 83] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75 07 50 E8 B1 D1 [FF FF] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35

3B C6 73 0F 8B 07 85 C0 74 02 FF [CC DE] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75 07 50 E8 B1 D1 [FA FE] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35

The RC4 keys strongly link at least 76 different samples in the Crowdstrike's intelligence library, all positively attributed to APT28/FANCYBEAR implants or loaders, aka GRU. The Ukrainian military's Android app may have been operationally less effective than initially portrayed. But

the effectiveness of the app is an issue entirely unrelated to the targeting itself. The forensic significance of quality artifacts found in the implants is strong, especially the cryptographic overlap.

Myers, Adam, interview with Thomas Rid, Washington, DC, 27 March 2017; see also Crowdstrike, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Washington, 22 December 2016.

[17] Bittman, Ladislav, *The KGB and Soviet Disinformation. An Insider's View*. Washington: Pergamon-Brassey's, 1985, p. 50–51.

[18] Russian intelligence agencies evolve their tradecraft at a fast pace, making it hard for network defenders to keep up with. Just this week, news emerged that APT29 is abusing Tor Hidden Services for controlling attacks against that likely target US government and think tanks. See FBI, "Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat," Washington, DC: FBI Cyber Division, 11 May 2016, p. 3. For background, Eduard Kovacs, "OnionDuke APT Malware Distributed Via Malicious Tor Exit Node," *Security Week*, 14 November 2014. More recently: Matthew Dunwoody, "APT29 Domain Fronting With TOR," Fireeye, 27 March 2017.

[19] As many as 15 percent of Twitter accounts may be bots, which amounts to almost 50 million "users." One recent research project observed "a growing record of malicious applications of social bots." See Onur Varol et al, "Online Human-Bot Interactions: Detection, Estimation, and Characterization," Social and Information Networks, arXiv:1703.03107, 27 Mar 2017.

[20] Agayants, quoted in Bittman, *The KGB and Soviet Disinformation*, p. 70.